

Flash cookies: is the EU about to make them crumble?

Today, "cookies" are an essential function of many websites seeking to sell products and services to their users; however, since their "birth", cookies have created privacy issues due to their user behaviour tracking capabilities. With the implementation of the Electronic Communications Directive,*1 website operators were finally forced to sit up and take account of privacy concerns, ensuring that users of their websites were provided with "clear and comprehensive information about the purposes of the storage of, or access to, that information" and ultimately, provide the user with the opportunity to refuse such storage of, and/or access to, that information.

We have however moved onto the next generation of cookies, the "flash cookie": (albeit they have in fact been around now for several years), and with it sees the resurrection of an "old" problem - "does the user know they are there and how can they get rid of them", along with the creation of some new problems.

The current state of compliance?

A recent academic study has found that over half of the top 100 websites are retaining user information through flash cookies without permission and thus are failing to comply with the *Electronic Communications Directive* and the *Privacy Directive*.*2

The study, by researchers at the Berkeley School of Law, at the University of California in Berkeley*3, will be of particular concern to those who try to delete cookies as a means of keeping their internet browsing patterns private. Flash cookies differ from the HTTP cookies which users are able to delete on request, in that they remain largely undetected by privacy settings on software such as Internet Explorer and Firefox.

What makes a "flash cookie" so special?

A cookie is simply a small piece of text stored on a user's web browser.

*"Cookies are small files which are stored on a user's computer. They are designed to hold a modest amount of data specific to a particular client and website, and can be accessed either by the web server or the client computer. This allows the server to deliver a page tailored to a particular user or the page itself can contain some script which is aware of the data in the cookie and so is able to carry information from one visit to the website (or related site) to the next".*4*

A flash cookie is fairly similar and does a similar job; however it can store more information and is much harder to detect.

*"Flash cookies are a new way of tracing your movement and storing a lot more information about you than with normal cookies. One major disadvantage of flash cookies is that you can't locate them in your browser. They are not shown in the list of cookies that you can see when you take a look at the cookies that are currently saved in your web browser Normal HTTP cookies can't save more than four Kilobytes of data while flash cookies can save up to 100 Kilobytes." *5*

Flash cookies, which are also known as Local Shared Objects, originate from coding found in Adobe's Flash media player. This is an application which is used by the vast majority of commercial websites that feature animations or videos. So you should probably assume that NOTES most of the time they are there!

The Berkeley study found that 54 of the top 100 websites used flash cookies which track user activity, and within that number, only four websites actually mentioned the use of flash technology for tracking purposes in their privacy policy. Although many flash cookies are beneficial to the user and enhance the overall user experience on a website (the most common flash cookie found on the sites was to store preferred volume settings), the researchers were surprised to find a high number of cookies were labelled "user ID" or similar - these cookies typically store unique identifiers which assist in user tracking.

What degree of sophistication?

In several cases where researchers attempted to delete or block HTTP cookies on flash-enabled sites, the flash cookies continued to trace user data and in some cases even "re-spawned" the deleted information upon the next visit to the site. This re-spawning was possible because some of the flash cookies had the same data values as the HTTP cookies, so in effect the flash cookies acted as a back-up on the computer system once the HTTP cookies had been removed. This instance even occurred across multiple domains, for example; a flash cookie originating from the online advertiser ClearSpring was found to re-spawn HTTP cookies on the websites of AOL, Mapquest.com and Answers.com. In addition, flash cookies even managed to subvert privacy settings on websites belonging to the Network Advertising Initiative (NAI). NAI websites offer users an opt-out via their own cookies, but in one case involving a Quant- Cast flash cookie, the flash cookie returned after deletion upon the next visit to the website, whereas the NAI opt-out cookie did not.

The Berkeley researchers concluded that only "sophisticated" user with knowledge of the different storage settings for flash cookies would even be aware of them and be able to manage them. This means that many individuals will be having their privacy breached without their knowledge every time they visit a webpage. It is perhaps of even greater concern in this respect because of the larger storage capacity and duration of flash cookies compared to HTTP cookies - with the potential for flash cookies to store up to 25 times more data, and the fact that flash cookies do not automatically expire over time, websites have, and will continue to acquire, much larger quantities of data than the average computer user would be aware of.

Another fundamental problem arising from websites' use of flash media, the researchers discovered, was the inability of some of these websites to function correctly once third-party content has been disabled - nine of the sites surveyed were unable to display their flash content - thus creating yet another disincentive for users who are trying to delete invasive cookies.

European data protection requirements

Any company which is utilising flash cookies to store user data is potentially in breach of European data protection laws, and care should be taken to mention this process when drafting your website privacy policy.

There are (in general) two pieces of European legislation which website providers require to comply with when using HTTP cookies and flash cookies; *the Electronic Communications Directive* and the *Privacy Directive*.

Whilst the Electronic Communications Directive acknowledges cookies as a:

*"legitimate and useful tool . . . their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using". *7*

and importantly:

*"(u)sers should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment". *8*

These two Directives provide a website operator with a framework within which to operate lawfully, where they step out with that framework they will be in breach of both Directives.

Article 5 (3) of the Electronic Communications Directive provides that each Member State:

*"shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user". *9*

Thus each "user", a data subject, must be provided with sufficient information about what the cookies are used for (for example, traffic analysis and advertising) to enable him to come to an informed decision and either provide or not provide his consent to the processing ("consent" in this context being a form of consent as set out in the Privacy Directive and the requisite domestic legislation).

The right to refuse

The right to refuse*10 is generally provided for by way of an opt-out under which the web provider will (or should in theory) no longer deliver, for example, advertisements which have been tailored to your web preferences and usage patterns. How the user is/was provided with this information and opt-out has been left open to interpretation and website operators across Europe have tended to put in place an "easy to find" Privacy Policy, within which the relevant information has been placed.

Website operators across Europe would appear to take the approach that to seek consent first would impact adversely on "usability" and therefore placing the details and opt out information in a privacy policy - which is usually a click (or two) away - is seen as a more straightforward approach and is one which doesn't seem to across Europe. Indeed in the UK, guidance issued by the Information Commissioner supports this approach.

The issue of flash cookies is however just one part of an increasingly prominent debate on the role of behavioural advertising generally and the means by which we choose to regulate it. In both the UK and in Europe, legislators have recently spoken out against allowing standard practices in behavioural advertising to continue.

Opt in or opt out?

In October of this year, the UK's All Party Parliamentary Communications Group (ApComms) published a report^{*11} into the regulation of internet service providers (ISPs) and other internet traffic issues, and has strongly recommended that new government regulations oblige ISPs to ask users to 'opt-in' to behavioural advertising processes *whilst* users are browsing. This is essentially a quite remarkable move away from how website operators deal with matters currently, where users must expressly 'opt-out' of having their browsing habits tracked, to continue.

The ApComms report followed an investigation into trials of a new ad-serving system called Phorm on BT's broadband network in the UK in 2006 and 2007. During the trial period, BT's customers were not given any indication that they were part of this process and were consequently unable to opt-out of having their data processed by Phorm, the company trialing the system. The European Commission has since heavily criticised the UK government for failing to adequately protect consumer's personal data, due to the manner in which the Electronic Communications Directive has been implemented by domestic legislation and is demanding that the UK make the necessary changes.

The EU itself is also close to passing a new law on cookies as part of the forthcoming EU telecoms reform package and should the EU's Council of Ministers and Parliament come to an agreement over one unresolved issue regarding file-sharing regulation, the package will come into force on 14 December 2009, complete with the new EU provisions relating to cookies. Again, the new law proposes that a user must explicitly choose to 'opt-in' to any website which intends to utilise behavioural tracking techniques.

Should the new EU telecoms reform package go through, it will no longer be sufficient to rely on a user's browser security settings as a means of evidencing a user's consent to the use of all cookies on a particular website (HTTP Cookies can usually be administered through a web browser's preference drop-down); all EU websites will be required to seek explicit consent from a user before applying their cookies on each webpage. Whilst it may not be, as ApComms acknowledged, "commercially convenient" to ask each user permission before serving each cookie, it is the most privacy-sensitive approach to the problem. A (big) headache nonetheless and yet another compliance issue for website providers across the EU.

These proposed changes to the law are likely to result in controversy and uncertainty, especially in terms of who will monitor and enforce the provisions, and how will this be done, given the scale of the task involved. Given the "annoyance factor" of having to read numerous messages, is it really practical for every user to read dozens of requests from website operators to serve cookies and then click "Accept" or "Reject" for each and every one? Europe to date has avoided this by taking the "privacy policy" approach to cookies!

To get rid of flash cookies and stop more appearing, instructions are available at <http://epic.org/privacy/cookies/flash.html>.

***Notes**

1. Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector.
2. Directive 95/46/EC of the European Parliament and Council of the 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862
4. <http://www.whatarecookies.com/>
5. <http://www.ghacks.net/2007/05/04/flash-cookies-explained/>
6. It is understood that Quant Cast has since the release of the Berkeley Report ceased using Flash cookies to re-spawn HTTP cookies (<http://www.privacylaw.proskauer.com/2009/09/articles/online-privacy/flash-cookies>). Posted 2 September 2009.
7. Preamble paragraph 25 Directive 2002/58/EC
8. ibid
9. ibid
10. The right to refuse does however have an exception in that those cookies which are provided on the basis of a service expressly re-requested by a “user” and are necessary for that service to be provided, then the web provider clear and comprehensive information to the user concerning that cookie.
11. “Can we keep our hands of the net?” Report of an inquiry by all the Party Parliamentary Communications Group, October 2009, http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf

Valerie Surgenor is a Senior Associate in MacRoberts. For more information please contact valere.surgenor@macroberts.com

This article featured in the World Data Protection Report in November 2009.

[See our website for full Copyright notice and Disclaimer.](#)

© MacRoberts LLP 2009